

**UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION**

UNITED STATES OF AMERICA)	
)	No. 3:24-CR-00151
v.)	JUDGE RICHARDSON
)	
MATTHEW ISSAC KNOOT)	
)	

UNITED STATES' NOTICE OF EXPERT TESTIMONY

The United States of America, by and through undersigned counsel, hereby files this Notice of Expert Testimony pursuant to Federal Rule of Criminal Procedure 16(a)(1)(G). In support thereof, the Government would respectfully show as follows:

I. Carla Rexing, FBI Special Agent:

The Government may seek to offer expert testimony by Federal Bureau of Investigation ("FBI") Special Agent ("SA") Carla Rexing. SA Rexing has been employed by the FBI since 2009, specifically as a special agent since 2017, and is currently assigned to the FBI Nashville Division as a member of the Cyber Task Force. SA Rexing is also a certified member of the FBI's Cellular Analysis Survey Team ("CAST"), which is a specialized unit within the FBI that provides technical expertise, case consultation, and instruction in the analysis of historical call detail records, cell site location information, and other forms of geolocation information.

The Government anticipates that if called as a witness, SA Rexing will offer expert testimony, in general terms and/or as applied in this case, regarding the extraction of data from electronic devices, including the cellular telephone seized from the defendant in this case, as set forth more specifically below:

1. SA Rexing will testify as to her training and experience, as detailed in her CV, including any training and experience associated with extracting data from cellular

devices. SA Rexing's curriculum vitae ("CV") is attached hereto as Exhibit A and sets forth her background, training, and experience, and identifies the trials and/or depositions in which she has testified during the previous four years. SA Rexing has not authored any relevant publications in the previous 10 years.

2. SA Rexing will testify about and explain the types of forensic extraction software available, the reliability of such software, and how such software is utilized to extract the data from electronic devices, including cellular telephones.

3. SA Rexing will testify about and explain what a cell phone extraction is; the process by which she conducts extractions from cell phones, and how the extractions are authenticated.

4. SA Rexing will testify about and describe what type of information can be extracted from a cell phone, including contacts, call logs, text messages, notes, photographs, videos, and location information. SA Rexing will further explain that such information may have metadata associated with it, including the date, time, and location associated with items of evidence recovered from these cell phone extractions as well as the type of camera used to take videos and/or photographs.

5. SA Rexing will testify that she conducted a forensic examination of the defendant's LG cell phone, model number LM-Q720. SA Rexing will testify regarding the procedures she followed, and equipment used, to extract the data from the defendant's cell phone and will identify the cell phone extraction. SA Rexing will identify the types of data recovered from the defendant's cell phone and explain that after she extracted the data from

the cell phone, she provided an extraction of that data to other law enforcement officers involved in the investigation of this case.

The bases for SA Rexing's conclusions are (1) her years of experience as a Special Agent, and particularly her experience as a member of the as the Cyber Task Force; (2) her specialized training and experience as a member of the FBI's CAST; (3) and her review of the facts of this case.

Consistent with the requirements of Federal Rule of Criminal Procedure 16(a)(1)(G)(v), SA Rexing has reviewed the foregoing disclosure and approves of the contents herein.



Carla Rexing
FBI Special Agent

05/09/2025
Date

II. Brian D. Jackson, FBI Supervisory Special Agent:

The Government may seek to offer expert testimony by FBI Supervisory Special Agent ("SSA") Brian D. Jackson. SSA Jackson has been a special agent with the FBI since March 4, 2007. Since April 5, 2010, SSA Jackson has been assigned to a cyber squad in the FBI's St. Louis Division investigating national security and criminal cyber threats. As a member of the cyber squad, SSA Jackson has received training in computer fraud and computer hacking and conducted investigations into various forms of online criminal activity. He is also familiar with the ways in which such crimes are commonly conducted. Additionally, SSA Jackson is a member of the FBI's Cyber Action Team (CAT), a rapid response fly team that responds to major cyber threats and attacks against critical infrastructure worldwide. From in or about August 2014 to the present day, SSA Jackson has investigated, among other things, Democratic People's Republic of North Korea

(“DPRK” or “North Korea”) cyber actors revenue generation through remote information technology (IT) work. On July 15, 2024, SSA Jackson was selected to be the supervisory special agent for the FBI St. Louis Field Office’s cyber squad.

The Government anticipates that if called as a witness, SSA Jackson will offer expert testimony, in general terms and/or as applied in this case, regarding North Korea revenue generation through remote IT work; the purpose of such revenue generation; how North Korean actors obtain remote employment; the technical and non-technical means North Korean actors used to obfuscate their true identity in order to obtain remote IT work; North Korean actors use of witting and unwitting third-party enablers to receive victim company laptops, login to said laptops, connect said laptops to the Internet, install remote desktop software on said laptops, and return said laptops to the employer upon the North Korean actor’s termination; North Korean actors deployment to other countries, including but not limited to China; North Korean actors use of Chinese telecommunications infrastructure; and North Korean actors use of online payment platform, including but not limited to Payoneer, as set forth more specifically below:

1. SSA Jackson is expected to testify as to his training and experience, as detailed in his CV, including any training and experience associated with his role investigating North Korea cyber actors’ revenue generation through remote IT work and his supervision of FBI Special Agents investigating the same. SSA Jackson’s CV is attached hereto as Exhibit B and sets forth his background, training, and experience. SSA Jackson has not authored any relevant publications in the previous 10 years, nor has he testified as an expert at any trial or deposition in the past 4 years.

2. SSA Jackson is expected to testify and explain the underlying cause(s) for North Korean revenue generation, including comprehensive trade and economic sanctions by the United States against North Korea, due to the national security threats posed by North Korea and its nuclear weapons program. SSA Jackson is expected to testify and explain the effect of such sanctions on North Korea and how, as a result, North Korea has sponsored various schemes to evade U.S. sanctions to generate funds for the regime. SSA Jackson is further expected to testify and explain that such schemes include remote IT work.

3. SSA Jackson is expected to testify and explain how North Korea IT workers generate revenue (that is, earns money) by posing as non-North Korean foreign and U.S.-based remote IT workers and surreptitiously obtain remote IT work from companies around the world, including in the United States. SSA Jackson is expected to testify that North Korea has sent IT workers to other countries, including but not limited to China, where they work in small team or cells to obtain remote IT positions at U.S. companies.

4. SSA Jackson is expected to testify and explain how North Korean IT workers obtain remote IT jobs by applying directly with U.S. companies and indirectly through online freelancing platforms, such as Upwork, that allow companies to advertise contracts for IT projects on which freelance IT workers can bid. SSA Jackson is expected to testify and explain how North Korean IT workers create and season fake personas that they use to apply for these jobs.

5. SSA Jackson is expected to testify and explain how North Korean IT

workers provide prospective employers with counterfeit, altered, or falsified documents, including identification documents, to hide their true identities. SSA Jackson is also expected to testify and explain that to obtain these documents North Korean IT workers commonly pay individuals and online criminal marketplaces for document forgery services. SSA Jackson is also expected to testify and explain how North Korean IT workers purchase or steal the personally identifiable information (“PII”), such as names, social security numbers, dates of birth, among other information, of U.S. persons and use that information to apply for remote IT positions. SSA Jackson is further expected to testify and explain how North Korean IT workers combine this stolen PII of U.S. persons with pictures of themselves to create fraudulent identity documents, to include driver’s licenses, passports, and visas, which they use to apply for remote IT positions. Based on a review of information associated with this case, SSA Jackson is further expected to testify and explain how Yang Di’s use of U.S. citizen Andrew M.’s PII to apply for and obtain remote IT work is consistent with a typical North Korean remote IT work scheme.

6. SSA Jackson is expected to testify and explain how North Korean IT workers obfuscate their Internet Protocol (IP) address, identities, locations, and nationality through sophisticated technical means. Specifically, SSA Jackson is expected to testify and explain what virtual private networks (“VPNs”) and virtual private servers (“VPSs”) are and how North Korean IT workers use them. SSA Jackson is further expected to testify and explain that North Korean IT workers use VPNs to mask, among other things, their true geolocation by accessing the Internet through a VPN that makes it appear as though

they are accessing the Internet from a different location than the location in which they are physically located. SSA Jackson is expected to testify and explain what an IP address is, how IP addresses are assigned, and how devices utilize IP addresses to send and receive information across the Internet. SSA Jackson is also expected to testify what types of information investigators can glean from IP addresses and IP address logs, and how investigators can discern a criminal actor's true IP address when the actor loses or misconfigures their VPN connection. Based on a review of information associated with this case, SSA Jackson is expected to testify and explain how the Andrew M. persona's use of VPNs is consistent with the persona being operated by and IT work being performed by Yang Di and/or other co-conspirators. Based on a review of information associated with this case, SSA Jackson is further expected to testify and explain how certain IP addresses identified in this case resolving to China and/or Chinese infrastructure—and China Unicom in particular—is consistent with login activity by North Korean IT workers.

7. SSA Jackson is expected to testify and explain how North Korean IT workers use witting and unwitting third-party enablers physically located in the United States in furtherance of the fraudulent scheme to obtain remote IT work. SSA Jackson is expected to testify that these enablers may or may not know the North Korean IT worker's true identity—that is, the enabler may not know that the individual is North Korean. SSA Jackson is further expected to testify and explain how U.S.-based enablers provide their U.S. address to the North Korean IT workers, and how the U.S.-based enablers send and receive packages on the North Korean IT workers' behalf. Specifically, SSA Jackson will

explain how the IT workers tell the U.S. companies at which they've obtained employment that their mailing address is the enabler's U.S. address, causing the victim companies to send a company laptop computer and other devices to the enabler's address, thereby circumventing controls the companies had in place to prevent unauthorized individuals from being in possession of their devices. SSA Jackson is also expected to testify and explain how after receiving a laptop, the U.S.-based enablers unpackage the laptop, turn it on, connect it to the Internet, and use login credentials—that is, a username and password—provided by either the North Korean IT worker via a text-based communication platform or instructions provided by the victim company to log in to the victim company's laptop, and download and install remote access software, such as TeamViewer, AnyDesk, or Splashtop Streamer. Based on a review of information associated with this case, SSA Jackson is expected to testify and explain how the presence of remote desktop software on some of the victim company laptops and chat communications between the defendant and Yang Di are consistent with a U.S.-based enabler facilitating a North Korean IT worker's access to the victim company laptops.

8. SSA Jackson is expected to testify that many U.S. and other Western-based companies are aware of North Korean IT worker scams and undertake measures to prevent them. SSA Jackson is further expected to testify that these U.S. and other Western-based companies have policies in place that state their employees are not permitted to download or install software intended to circumvent the company's security controls, which includes software designed to enable remote access. SSA Jackson is also expected to testify and

explain how in some cases U.S.-based enablers ship the victim companies' laptops overseas, to locations including China, when they are unable to circumvent the company's security controls and install remote desktop software. SSA Jackson is also expected to testify and explain that the U.S.-based enablers will ship the laptops back to the U.S. company upon termination of the North Korean IT worker. SSA Jackson is further expected to testify and explain that the U.S.-based enablers performed these activities in exchange for a fee, which is typically paid to them through online money transfer and digital payment services. Based on a review of information associated with this case, SSA Jackson is further expected to testify and explain how the defendant's actions in this case—that is, receiving laptops, logging in to victim company laptops using credentials provided by Yang Di, connecting said laptops to the Internet, downloading remote access software, providing the remote access software codes to Yang Di, returning laptops to victim companies, negotiating payment for these services with Yang Di, and receiving payment through Payoneer—is consistent with that of a U.S.-based enabler of North Korean remote IT worker schemes.

9. SSA Jackson is expected to testify and explain how North Korea IT workers create accounts with online payment platforms that specialize in facilitating cross-border business-to-business payments, cross-border wire transfers, online payments, and refillable debit card services, such as Payoneer. SSA Jackson is expected to testify and explain how North Korea IT workers use these online payment accounts to obtain correspondent bank accounts, which the North Korean IT workers provide to their U.S. employers so that they

can receive direct deposits. SSA Jackson is further expected to testify and explain how North Korean IT workers launder the funds paid into these online payment platforms to and through other online payment platform accounts and ultimately to banks overseas, including in China. Based on a review of information associated with this case, SSA Jackson is expected to testify and explain that the utilization of Payoneer by the defendant and Yang Di to send and receive payments is consistent with a North Korean remote IT work scheme.

10. SSA Jackson's testimony is expected to include a discussion of the *modus operandi* of North Korean IT workers, including common techniques to obfuscate their identities in order to obtain and maintain employment. SSA Jackson will explain how law enforcement can de-anonymize North Korea actors through review of overlapping online accounts, online payment returns, and online infrastructure to include IP addresses.

The bases for SSA Jackson's conclusions are (1) his years of experience as a Special Agent and Supervisory Special Agent, investigating, among other things, North Korean cyber actors' revenue generation through remote IT work; (2) and his review of the facts of this case.

Consistent with the requirements of Federal Rule of Criminal Procedure 16(a)(1)(G)(v), SSA Jackson has reviewed the foregoing disclosure and approves of the contents herein.



Brian D. Jackson
FBI Supervisory Special Agent

05/09/2025
Date

III. Andrew McDole, FBI Computer Scientist:

The Government may seek to offer expert testimony by Federal Bureau of Investigation (“FBI”) Computer Scientist (“CS”) Andrew McDole. CS McDole has been employed by the FBI as a CS since August 16th, 2021 and is currently assigned to the FBI Nashville Division. CS McDole is an FBI trained computer scientist with a background in digital forensics, internet traffic analysis, computer operating systems, and data extraction. He has experience analyzing complex computer crimes involving both computer fraud and computer hacking.

The Government anticipates that if called as a witness, CS McDole will offer expert testimony, in general terms and/or as applied in this case, regarding the forensic imaging of data from computers, including the desktop computer seized from the defendant in this case; the purpose of remote desktop software; how cyber criminals use remote desktop software; how remote desktop software modifies a computer; the purpose of VPNs; how cyber criminals use VPNs; what an IP address is and how investigators use IP addresses, as set forth more specifically below:

1. CS McDole will testify as to his training and experience, as detailed in his CV, including any training and experience associated with extracting data from computers. CS McDole’s curriculum vitae (“CV”) is attached hereto as Exhibit C and sets forth his background, training, and experience, and identifies the trials and/or depositions in which he has testified during the previous four years.
2. CS McDole will testify about and explain the types of forensic imaging techniques and software available, the reliability of such techniques and software, and how

such techniques software are used to obtain data from electronic devices, including desktop computers.

3. CS McDole will testify about and explain what a forensic image is; the process by which he obtains a forensic image, reviews the forensic image, and how the image is authenticated.

4. CS McDole will testify about and describe what type of information can be imaged from a computer, including documents, images, IP addresses, browsing history, emails, log information, usernames, passwords, notes, photographs, videos, and location information. CS McDole will further explain that such information may have metadata associated with it, including the date, time, and location associated with items of evidence recovered from the forensic images.

5. CS McDole will testify that he conducted a forensic examination of the defendant's desktop computer, identified by the black case with glass panel consisting of custom computer hardware using digital write-blockers and Linux operating system-based digital triaging methods. CS McDole will testify regarding the procedures he followed to extract data from the defendant's computer and will identify the computer files. CS McDole will identify the types of data recovered from the defendant's computer and explain that after he extracted the data from the computer, he provided a copy of the extracted data to other law enforcement officers involved in the investigation of this case.

6. CS McDole is expected to testify and explain what remote desktop software is. Specifically, CS McDole will explain the purpose of remote desktop software; how a

user obtains (downloads) remote desktop software; how a user installs remote desktop software; how a user provides others with access to the computer upon which the remote desktop software has been downloaded; the degree of control granted to the remote user by the remote access software; how cyber criminals use remote desktop software; and how the installation of remote desktop software modifies a computer.

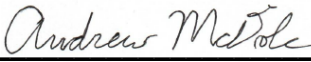
7. CS McDole is expected to testify and explain what a VPN is. Specifically, CS McDole will explain the purpose of a VPN; how a user obtains (downloads) VPN software; how a user installs VPN software; the effect that utilization of a VPN has on a user's IP address and other geolocation data; how cyber criminals use VPNs to obfuscate their true location; and how law enforcement can discern a cyber criminal's true IP address when the actor loses or misconfigures their VPN connection.

8. CS McDole is expected to testify and explain what an IP address is; how IP addresses are assigned; how devices utilize IP addresses to send and receive information across the Internet; how IP addresses can be used by law enforcement to track activity by users, how law enforcement uses IP addresses to determine geographical location of users in correlation with time of day; how cyber criminals attempt to obscure their real IP address to, among other things, hide true location; how cyber criminals use VPNs to obscure their real IP address; and how IP addresses appear in logging systems commonly used in work-from-home situations.

The bases for CS McDole's conclusions are (1) his years of experience as a Computer Scientist; (2) his training in the field of computer science and digital forensics; and (3) his review

of the facts of this case.

Consistent with the requirements of Federal Rule of Criminal Procedure 16(a)(1)(G)(v), CS McDole has reviewed the foregoing disclosure and approves of the contents herein.



Andrew McDole
FBI Computer Scientist

05/09/2025
Date

IV. Request for Notice of Defendants' Expert Testimony

The government hereby requests, pursuant to Fed. Crim. R. (16)(b)(1)(C) disclosure of a written summary of expert testimony the defendant intends to use as evidence at trial or at any hearing. This summary must describe the opinions of the witness, the bases and reasons therefore, and the witnesses' qualifications.

CONCLUSION

The Government asserts this notice and the discovery provided to the defendant satisfy the requirements of Rule 16(a)(1)(G) of the Federal Rules of Criminal Procedure. If after viewing this notice and any attachment(s), the defendant requests further information or has concerns under Rule 16, the Government requests the defendant advise as to what further information is necessary to prepare for trial. The Government will supplement this notice if it discovers additional evidence that will be presented through expert opinion.

Respectfully Submitted,

ROBERT E. McGUIRE
ACTING UNITED STATES ATTORNEY
MIDDLE DISTRICT OF TENNESSEE

SUE J. BAI
HEAD OF THE
NATIONAL SECURITY DIVISION

Date: May 9, 2025, 2025

By: /s/ Gregory J. Nicosia, Jr.
GREGORY J. NICOSIA, JR.
D.C. Bar No. 1033923
Trial Attorney
National Security Cyber Section
National Security Division

JOSHUA KURTZMAN
Assistant United States Attorney
Middle District of Tennessee

CERTIFICATE OF SERVICE

I hereby certify that on May 9, 2025, a true and correct copy of the foregoing document was filed with the Clerk of the Court by using the CM/ECF system, which will send a Notice of Electronic Filing to counsel for defendant.

/s/ Gregory J. Nicosia, Jr.
GREGORY J. NICOSIA, JR.
D.C. Bar No. 1033923
Trial Attorney
National Security Cyber Section
National Security Division